

**Statement
of
Christopher J. Christie
United States Attorney
for the
District of New Jersey**

Before the

**Committee on Energy and Commerce
Subcommittee on Oversight and Investigations**

July 10, 2006

“Sexual Exploitation of Children over the Internet”

Chairman Whitfield, Ranking Member Stupak, and distinguished members of the Subcommittee, thank you for inviting me to testify before you today about my office’s prosecutions of cases involving the sexual exploitation of children on the Internet, including the RegPay case, in which we prosecuted both producers and consumers of child pornography.

Introduction

As this Subcommittee is already no doubt aware, the advent of the Internet has led to a vast proliferation in the availability and prevalence of child pornography in today’s society. The possession and distribution of child pornography were once relatively rare crimes relegated to those who would frequent certain underground adult bookstores or attempt to order obscure magazines from overseas. The Internet has dramatically changed that by making child pornography easy to produce and distribute, while also making it readily available to those inclined to seek out this material from their own home. Sadly, thousands of individuals who are sexually attracted to children now have ready access to images and videos depicting the sexual exploitation and molestation of children. Moreover, unscrupulous and opportunistic individuals both here and especially abroad have seized the opportunity to market access to child pornography in an industry that provides huge profits and relatively low overhead costs. It is probably accurate to say that the number of individuals in this country who have intentionally obtained access to or traded images of child pornography within the last six-month period outstrips the number for a similar six-month period from 15 years ago by at least a hundredfold. In addition, the Internet has also become an avenue for child predators to seek out and communicate with children in the seeming anonymity of chat rooms.

Needless to say, this sea change has created a tremendous challenge for law enforcement -- one that requires law enforcement to adapt quickly to a rapidly changing landscape and to search for innovative ways to identify and apprehend offenders. It has also put a premium on law

enforcement officers with technological and computer expertise.

Law enforcement efforts to interdict Internet-based child exploitation crimes are largely dictated by the nature of the offense, which can be loosely grouped into two categories: child pornography offenses and child exploitation cases. The former type of investigation is more heavily dependent on technological expertise and forensic investigation, while the latter is typically dependent on the capacity of an individual agent to convincingly portray himself or herself as a minor who is susceptible to advances by on-line predators.

To understand child pornography offenses and the efforts of law enforcement to effectively investigate them, it is necessary to understand the nature of child pornography on the Internet. Much of the proliferation of child pornography can be traced to the existence of numerous commercial websites that offer access to child pornography for a monthly fee. During the past ten years, hundreds of websites, many based in Eastern Europe, have appeared on the Internet. These sites typically require a subscriber to submit various information including billing information, whether it be via credit card or some other on-line payment service such as E-Gold. Law enforcement efforts to interdict these websites and to apprehend both those who operate them and those who subscribe to these sites has proven a formidable task, but there have been notable successes. Foremost among these successes has been the RegPay investigation which represented the collaboration of a number of federal agencies, including the Federal Bureau of Investigation (FBI), the Department of Homeland Security's Immigration and Customs Enforcement (ICE), the Internal Revenue Service Criminal Investigations, and the Postal Inspection Service, in conjunction with the United States Attorney's Office for the District of New Jersey and the Child Exploitation and Obscenity Section in the Department's Criminal Division (CEOS). It is also illustrative of how the federal government can successfully target the commercial child pornography industry at both the level of the producer and the consumer.

The RegPay Case

The RegPay investigation, which began in early 2003, represented the first large-scale effort to target the operators of commercial websites offering access to child pornography over the Internet and to track the financial trail created by those who profit from this industry. In the early part of that year, federal agents made undercover purchases of monthly subscriptions to numerous child pornography websites in an effort to track down the producers of the material and the operators of the sites. The investigation revealed that a company based in Belarus, which called itself RegPay, operated several commercial child pornography websites and processed credit card fees for more than 50 other similar sites. The investigation also determined that credit card payments for access to these sites were being processed through a company based in Ft. Lauderdale, Florida known as Connections, USA. Agents also executed search warrants on computer servers based in Texas and Virginia that RegPay had leased, and recovered extensive databases documenting credit card transactions involving approximately 90,000 customers worldwide. Armed with this information the investigation pursued two paths, aimed at, on the one hand, the operators of RegPay and those who processed their transactions, and, on the other hand, the consumers who purchased access to the site.

To pursue the operators of RegPay, agents first executed a search warrant at Connections, USA in Ft. Lauderdale. Upon executing the search warrant, agents learned of an ongoing financial dispute between Connections, USA and the operators of RegPay relating to an outstanding debt of more than one million dollars supposedly owed to RegPay. Agents were able to assume the role of Connections, USA to broker a meeting in Paris between the operators of RegPay and Connections, USA, ostensibly to resolve the ongoing dispute and to set the groundwork for future financial cooperation between the companies. This ruse led to the arrest of two Belarussians in Paris while a third individual was apprehended while vacationing in Spain at the same time. All three were extradited to New Jersey to face charges relating to the production and distribution of child pornography. All three pled guilty on the eve of trial in February of 2005 before the Honorable Dennis M. Cavanaugh of the United States District Court of New Jersey. The two principals of RegPay, Yavor Zalatarou and Aliaksandr Boika, are expected to be sentenced later this month. They face presumptive sentences in the range of 25 to 30 years. In total, 9 individuals pled guilty in the District of New Jersey for their involvement in operating or supporting RegPay's business operations, including three individuals from Connections, USA as well as three California-based individuals involved in the laundering of RegPay's proceeds. One of these latter individuals, Yaroslav Grebenshikov, admitted that in late June 2003, he assisted individuals associated with Regpay in the formation of LB Systems - a company created to assist Regpay and others in Belarus to process credit card sales for previously approved transactions involving child pornography - as well as the opening of a bank account, both of which he used to transfer more than \$200,000 in funds associated with RegPay to banks in Latvia.

Simultaneously, in what was dubbed Operation Falcon, agents pursued the consumers of child pornography by following the transaction history of those who had gained access to the RegPay-supported child pornography websites. By comparing the transaction data obtained via the search warrants conducted on the servers in Texas and Virginia with credit card records, agents were able to seek search warrants for numerous individuals throughout the United States. Leads were also distributed worldwide to pursue those who knowingly received and possessed child pornography. Through February of 2006, the RegPay investigation had resulted in 341 federal, state and local arrests in the United States and approximately 703 additional international arrests. In the District of New Jersey alone, more than 50 individuals were charged federally with possession of child pornography. The New Jersey defendants included teachers, a pediatrician, a psychologist, a retired minister and, perhaps least surprisingly, several individuals who had been convicted of sex offenses against minors, including a former school principal.

Recidivist Offenders

This latter category illustrates the importance of pursuing the consumers of child pornography because, among other reasons, the link between those who seek out child pornography and those who molest children is substantial and disturbing. Of the approximately 52 New Jersey targets charged federally in New Jersey, 5 had prior convictions for sexual offenses against minors. In addition, 3 other defendants, when confronted by ICE agents conducting searches on their computers, admitted to molesting a total of at least 14 children, while two

defendants, including one of the convicted sex offenders, admitted to attempting to meet minors in on-line chat rooms. What cannot be known is how many others of those who were arrested had molested in the past but chose not to reveal this to authorities. While it is uncertain what percentage of those who gain access to child pornography act out upon their impulses, it is clear that a significant percentage do and common sense dictates that the exposure to child pornography encourages this behavior. For example, a study completed in 2000 by the Director of the Sex Offender Treatment Program at the Butner Federal Correctional Complex in North Carolina revealed that of 54 inmates convicted of child pornography offenses, 79.6% of them admitted that they had also molested significant numbers of children.

Harm to Exploited Children

Furthermore, the proliferation of child pornography websites and the great profits reaped by their operators fuels a market for the production of new and often hard-core child pornography. In short, the market in child pornography directly leads to the exploitation and molestation of children from all over the globe, often for the purpose of commercial gain. Many of the victims are from Eastern Europe where a substantial percentage of child pornography is produced. Images and videos of American children are encountered with great frequency, however, because once a photograph of child pornography makes its way on to the Internet - something that can be accomplished with ease in the era of digital photography - control of that image is essentially lost, and commercial websites may include such images in the collections they offer on their sites. Sadly, the victimization of children forced to become the subjects of child pornography thus continues as the image travels throughout the Internet. As Attorney General Gonzales noted recently, “[child pornography] is not a victimless crime. Most images today of child pornography depict actual sexual abuse of children. Each image literally documents a crime scene.”

The Evolving Landscape and Law Enforcement’s Challenge

As with most sophisticated criminal enterprises, the purveyors of child pornography adapt to law enforcement techniques, thus forcing investigators to adjust to an ever-changing landscape. The commercial child pornography industry has evolved even since the RegPay investigation. For instance, child pornography websites are not as easily located on the Internet by the uninitiated as was the case three to four years ago. While this may reduce the number of individuals subscribing to these sites, it also makes them harder for law enforcement to locate and identify. Moreover, the operators of these sites are increasingly sophisticated in hiding their own identities and whereabouts. They accomplish this both technologically - by making their operations more difficult to trace through the use of such software as anonymizers - and by insulating themselves through the use of sham Internet-based companies and other third parties through which they funnel their profits from the child pornography websites. Moreover, they lease server space typically through the use of stolen identities, and the companies that lease the space to them frequently do not realize the true content of the website they are helping to host. Perhaps the greatest challenge to bringing these individuals to justice, however, stems from the concentration of such operations in Eastern Europe, typically in the break-away Soviet republics such as Belarus. Most of these countries do not have extradition policies with the United States, and the knowledge

of the fate of the RegPay defendants makes the likelihood that operators of similar sites will venture outside the relative safety provided by the borders of their home country remote at best. Widespread corruption amongst Government officials in some of these countries significantly reduces the chances that they will face meaningful prosecution in their homeland.

These obstacles mean that curbing demand for child pornography will be increasingly important in combating the proliferation of this material. Techniques including electronic surveillance and the execution of search warrants on servers both domestically and abroad provide a deterrence effect for those who might seek child pornography through online commercial websites. Law enforcement needs to send a clear message that individuals who subscribe to these websites and contribute to the molestation of children across the globe run a substantial risk of facing significant jail time any time they hit the "JOIN NOW" button for one of these sites. As I speak here today, even though child pornography websites are harder to locate than before, there are still thousands of Americans who attempt to subscribe to child pornography websites every month. Law enforcement can and will play a significant role in bringing such individuals to justice.

Alternative Distribution Methods

While I have spoken so far primarily about the role of commercial websites in the proliferation of child pornography, it is important to realize that a great deal of child pornography gets distributed on the Internet through individuals who trade such material with one another. Additionally, peer-to-peer software such as Kazaa and Limewire may be abused by those with a mutual interest in child pornography to share their respective collections with one another if they belong to the same network of computers. Child pornography may also be distributed through attachments to e-mail. Individuals with an interest in child pornography may frequent certain chat rooms from which they will exchange collections. In addition, certain individuals may establish on their home computer what is known as an F-Serve on which they establish a collection of child pornography that can only be accessed by those who upload images of child pornography to the F-Serve first - thereby preventing law enforcement from gaining access while expanding the F-Serve operator's own collection.

All of these methods for distributing child pornography cause many of the same harms as posed by commercial child pornography websites, namely, the continued victimization of the children depicted and the encouragement of those with pedophilic impulses to act upon them. Law enforcement can identify many of the individuals involved in these forms of distribution through a variety of techniques. For instance, certain programs can be run which search computers that are connected through the same network for a particular image as defined by its hash value. This enables law enforcement to identify individuals who have particular images of child pornography on their computers and may establish sufficient probable cause for search warrants. In addition, forensic examination of an individual's computer that has been seized may reveal e-mail communications with other individuals who have sent and received child pornography from the seized computer. In this regard, traditional cooperation from a defendant who has distributed child pornography through these means may lead to the identification and arrest of numerous others.

Interstate Traveler Cases

In addition to investigations involving child pornography, the FBI plays a vital role in preventing and even interdicting child exploitation crimes so long as there is some interstate nexus to provide federal jurisdiction. The best known example of this type of investigation is the so-called enticement or “traveler case,” which has been recently well documented on a series of “Dateline NBC” episodes. Across the country, too many of our children have been lured by child abusers through contacts in chat rooms that are allegedly closed to adults. Some of these interstate travelers also take pictures of the minors they molest and sometimes abduct, and then post the child pornography online. This type of investigation requires an undercover agent to enter an Internet chat room where older men are likely to be interacting with minors. The undercover agent will engage in a series of chats to determine if the other individual is an adult seeking sexual contact with the undercover whom he believes to be a young teenager. As the chats progress, the older male may decide to travel to the location of the minor in the hopes of renting a nearby motel room or making similar arrangements. If the older male travels across state lines to meet the minor, the case may be taken federally. While many “traveler cases” may be prosecuted at the state level, federal traveler cases are not uncommon. For instance, the District of New Jersey is currently prosecuting a case where a doctor from a prominent Philadelphia hospital traveled to Hackensack, New Jersey expecting to meet a 14-year old girl with whom he intended to have sexual relations. Such “traveler cases” often involve actual minors whom the traveler intends to sexually abuse. For example, the District of New Jersey recently secured a conviction of a Florida man who traveled to New Jersey to have sex with a 13-year old girl. ICE agents, who did not initially know the identity of the intended victim, trailed the defendant and observed him following a school bus in an effort to find the girl whom he had met over the Internet. The agents were able to interdict this crime before the defendant, who was in possession of a stun gun and alcohol, contacted the victim. It is likely that such crimes, however, are greatly under reported by the young and confused victims.

Sex Tourism Cases

Another, albeit less common type of child exploitation case that may involve the Internet arises out of sex tourism investigations wherein the defendants are individuals who travel overseas to have sex with minors, or who organize such trips. These trips frequently involve travel to southeast Asia. Sex tour operators catering to pedophiles tend to be discreet and are difficult to infiltrate because they are usually extremely wary of law enforcement. If successful, however, these cases may not only lead to the apprehension of the tour operator, but his prior clients as well. Because of the international nexus of these violations, ICE often acts as the primary federal law enforcement agency responsible for conducting such investigations. ICE has conducted many successful child sex tourism investigations and works closely with CEOS, the U.S. Attorney's Offices, as well as federal, state and local law enforcement agencies.

The District of New Jersey is currently prosecuting one such case where the defendant operated a website advertising sex tourism. The website did not specifically advertise that its tours were catered toward minors, but it included pictures of girls in various states of undress,

some of whom clearly appeared to be underage. The investigation involved undercover Internet chats followed by meets wherein undercover agents posed as customers seeking to have sex with underage girls upon arrival in the Philippines. The defendant initially indicated that he would not talk about minors until the group arrived in the Philippines, but he gradually opened up to the point where he admitted to having sex with minors himself.

Project Safe Childhood

All of the investigations that I have described so far will be bolstered by the Department of Justice's recently launched Project Safe Childhood initiative designed to coordinate the efforts of federal agencies and U.S. Attorneys' Offices with state and local law enforcement. This initiative is designed to help coordinate national child pornography investigations, train additional federal, state and local law enforcement in pursuing computer-based investigations and raise community awareness of the dangers of the Internet for children. The initiative is also designed to increase federal involvement in many of these investigations, especially where state laws provide little deterrence for offenders. This latter point is clearly evident in New Jersey where possession of child pornography regularly results in sentences of 2 to 3 years if prosecuted federally but carries with it a presumption of a probationary sentence under state law.

I am proud that the District of New Jersey has been a leader in pursuing child exploitation offenses on a national level, as evidenced by the RegPay case, which represents one of the most successful child pornography investigations in the nation's history. Most importantly, Project Safe Childhood will ensure that every state and every district has properly trained law enforcement officials who can vigorously pursue predators and similar offenders, when supplied with appropriate leads, and that these investigations will realize even greater success in the future.

I should also note that the District of New Jersey's experience in pursuing RegPay and other similar investigations demonstrates that the number of child pornography and other child exploitation offenders is quite simply staggering, and that it behooves law enforcement offices - whether they be the prosecuting authority or the investigative agency - to devote greater resources and personnel to these investigations. The RegPay investigation demonstrates that a few well-trained and dedicated law enforcement officials can make a major impact and provide prosecutors and agents in their own and other districts with large numbers of dangerous offenders to pursue and bring to justice. Unfortunately, sometimes our own American youth are the victims of traffickers in this country who lure youth from their communities and sell them for prostitution in other jurisdictions, offering them for sex at truck stops, conventions, and on the streets of our cities.

Human Trafficking

I would be remiss if I did not mention that the impact of federal law enforcement's efforts to protect children is not limited to investigations focused on the Internet. One type of crime that frequently entails the exploitation of minors are those involving human trafficking, whether they involve forced labor or sex trafficking. Many of the victims of this type of deplorable crime are

minors, and they are often sexually exploited on a commercial basis. Human trafficking is a crime that has been with us for many years, but continued largely unnoticed until the passage of the Trafficking Victims Protection Act of 2000, authored by a strong, committed group of legislators including Representative Christopher Smith, from my home state of New Jersey. That legislation recognized that many individuals, typically young female immigrants, were being smuggled into the United States and forced to work in demeaning conditions or in prostitution. Since the passage of that legislation, numerous trafficking cases have been brought throughout the United States, and the District of New Jersey has once again been one of the leaders in pursuing these types of cases.

In 2002, for example, this Office brought the case of *United States. v. Jimenez-Calderon* which led to the convictions of two women for their role in forcing several juvenile Mexican girls to work as prostitutes in Plainfield, New Jersey. The defendants received sentences of approximately 17½ years each. In 2005, this office indicted the case of *United States. v. Luisa Medrano, et al.*, which involved the smuggling into the United States of young Honduran females, some as young as fourteen, after they had been promised legitimate waitressing jobs to lure them into the country. Upon arrival in Union City, New Jersey, these girls were forced to work six or seven days per week at bars catering to male immigrants where they were pressured to perform sexually provocative dances for the customers and ply them with alcohol. The victims were also required to live at specific residences and had their movement greatly restricted until their smuggling debts were paid off in full. Many of these juveniles were sexually exploited during the smuggling process that brought them to New Jersey.

Even more recently, the District of New Jersey has brought various charges against a number of defendants for their involvement in prostitution activities in Hudson County and elsewhere. These defendants are primarily members of the Notario family from San Miguel Tenancingo, the trafficking capital of Mexico. The investigation has identified numerous trafficking victims who were put to work as prostitutes in various brothels along the East Coast after having been smuggled in from Mexico. Among these identified victims are at least three juveniles. Thus, the pursuit of human trafficking cases often represent yet another means by which law enforcement identifies and dramatically assists sexually exploited minors.

Conclusion

In conclusion, the dangers of the Internet in the proliferation of child exploitation crimes cannot be underestimated. The Attorney General has recognized that “we are in the midst of an epidemic in the production and trafficking of movies and images depicting the sexual abuse of children,” and the need for law enforcement to respond rapidly and forcefully cannot be more clear. With proper coordination and the cooperation of federal, state and local authorities, the Internet can be made far safer for the children of this country. Law enforcement must create an environment in which sexual predators fear the Internet as a dangerous place that may likely land them in prison for a significant period of time. The RegPay investigation - especially with the advent of Project Safe Childhood - provides a model for law enforcement agencies throughout the country to pursue child exploitation cases with the knowledge that the offenders who are identified will be vigorously investigated and prosecuted.

Mr. Chairman, I again thank you and the Subcommittee for the opportunity to speak to you today, and I would be pleased to answer any questions the Subcommittee might have.